

BEFORE THE
Department of Defense
Washington, DC 20554

In the Matter of

Notice of Proposed Rule with Requests
for Comment

Proposal to amend 48 CFR parts 204,
235, and 252

Amendments to address requirements
for preventing unauthorized disclosure of
export-controlled information and
technology under DoD Contracts.

DFARS Case 2004-D010

To: Defense Acquisition Regulations Council, Department of Defense

COMMENTS OF EADS NORTH AMERICA DEFENSE COMPANY

Introduction

1. EADS North America Defense Company (the "Company"), hereby comments on the above captioned Notice of Proposed Rule with Request for Comments ("NPR"), in which the Department of Defense ("DoD") proposes to amend Parts 204, 135 and 252 of Title 48 Code of Federal Regulations ("CFR") to address requirements for preventing unauthorized disclosures of export-controlled information and technology under DoD Contracts.

2. EADS North America Defense Company (“Company”) is incorporated in California and has its principal place of business in Arlington, Virginia. The Company has several contracts with DoD, both as contractor and subcontractor, and therefore is an interested party in the above captioned proceeding.

General Comments

3. We heartily endorse the intention of the proposed rulemaking. Compliance by contractors with the export control laws and regulations is an extremely important obligation of all contractors.

4. However, we believe that making export compliance a contract term is an extremely complicated matter and introduces numerous issues that are not adequately covered in the proposed rule, which issues probably should not be addressed by contract terms.

5. The Bureau of Industrial Security (“BIS”) of the Department of Commerce (“DoC”) has the responsibility for enforcing the Export Administration Act of 1979¹ as extended by Executive Order 13222 (“EAA”) covering dual-use goods and has promulgated extremely long and complicated implementing regulations known as the Export Administration Regulations (“EAR”)².

¹ 50 U.S.C. App. 2401 *et seq.*

² 15 CFR Parts 730 – 774.

6. The Directorate, Defense Trade Controls (“DDTC”) of the Department of State (“DoS”) has the responsibility for enforcing the Arms Export Control Act of 1976 (“AECA”)³ covering defense articles and has promulgated implementing regulations known as the International Traffic in Arms Regulations (“ITAR”).⁴

7. The export control laws and regulations are extremely complicated and difficult. Technical violations are easily committed by the best intentioned and the best compliance oriented companies. The export compliance personnel employed by defense contractors are, of necessity, subject matter experts and are supported by specialized outside counsel also with subject matter expertise.

8. Likewise, BIS and DDTC have licensing, compliance and enforcement personnel that are required to be subject matter experts and receive extensive training. Senior licensing, compliance and enforcement officers have many years of experience in export control matters. Both agencies are headed by high ranking government officials, reflecting the gravity of the responsibility of these agencies for protecting national security and foreign policy interests of the United States.

9. The enforcement mechanisms employed by the BIS and DDTC have been developed over many years to account for the national security and foreign policy interests of the U.S. These enforcement mechanisms take into account all of the

³ 22 U.S.C. § 2751 *et seq.*

⁴ 22 CFR Parts 120 – 130.

subtleties of the export control laws and regulations and are the result of several decades of experience. The standards, procedures and enforcement results are well established and predictable and are understood by both government and industry.

10. DoD contracting officers, on the other hand, are not trained or well equipped to handle export control issues and we suggest that export control law and regulation compliance is not a responsibility that should be assigned to contracting officers.

11. Making export compliance a contractual term introduces an unexplored and not well understood risk of contractual breach. The contractual consequences of a minor or even a major violation of the export control laws and regulations are not defined. Application of the rules is likely to be uneven and inconsistent because of the lack of subject matter expertise and there is a real risk of inconsistency between DoD and the responsible agencies. Such a small thing as the use of language in the proposed rules that is different from the language used in the EAR and ITAR may introduce a very serious contractual risk that is unquantifiable.

12. On balance, it would appear to be more appropriate and less complicated to leave compliance with export control laws and regulations to the agencies of the federal government that have jurisdiction for enforcing such laws and regulations. Those agencies have the subject matter expertise and have mature enforcement/compliance personnel to properly adjudicate violations.

13. Nevertheless, the proposed rules are well intentioned. Consequently, the remainder of our comments will be directed to specific provisions of the proposed rules and are intended to reduce unnecessary contractual risk, reduce regulatory overlap and facilitate application to subcontractors and foreign contractors.

Proposed § 204.7301 Definition

14. No comment on proposed section 204.7301.

Proposed § 204.7302 General

15. The proposed section 204.7302 reads as follows:

204.7302

Export control laws and regulations restrict the transfer, by any means, of certain types of information and technology. Any access to export-controlled information or technology by a foreign national or a foreign person anywhere in the world, including the United States, is considered an export to the home country of the foreign national or foreign person. For additional information relating to the restrictions on export-controlled information and technology, see PGI 204.7302.

16. While it may be linguistically correct to say that the export control laws and regulations “restrict” exports (if it is understood that “restrict” means “limits”), we believe it would be more clear to say that the export control laws and regulations “prohibit unauthorized” exports of certain types of information and technology. This language, we suggest, more clearly puts the reader on notice that a prohibition (and possible legal ramification) is involved and that one must have an authorization before exporting. Both the EAR and the ITAR authorize exports of certain types of information and technology

without a license and provide for other types of exports to be authorized by the granting of a license.

17. We also suggest that the use of the term “access” is problematical. “Access” is not a term that is used in either the EAR or the ITAR. The correct term for determining if an export has taken place is whether technical data subject to the EAR has been “released” to a foreign national⁵ or whether technical data subject to the ITAR has been “disclosed” or “transferred” to a “foreign person” (as defined by ITAR).⁶

18. We suggest that it would be unwise to use language that is not the same as the language used in the EAR and/or the ITAR. The introduction of new or different language creates the possibility that a contractor could be found to be in breach of the contract terms but not be in violation of the export control laws and regulations that the contract terms are intended to further.⁷

19. Both the EAR and the ITAR regulate the “export” of certain types of information and technology. The term “export” is defined very carefully in the EAR and the ITAR. The term export is defined to include “deemed exports” as clearly indicated in the

⁵ See, EAR § 734.2(b)(2) (17 CFR § 734.2(b)(2)). BIS defines the term “release” at EAR § 734.2(b)(3) (17 CFR § 734.2(b)(3)). The term “foreign national” is not defined.

⁶ The terms “disclosing” and “transferring” are not defined in the ITAR. The term “foreign person” is defined in ITAR § 120.16 (22 CFR § 120.16).

⁷ It is possible to have access to technical data and not have a release, a transfer, or a disclosure. It should be noted that the requirements for technical data subject to the EAR and technical data subject to the ITAR are not the same as the requirements imposed by the National Industrial Program Operating Manual (“NISPOM”) for “classified information.” Access to “classified” information by unauthorized persons must be reported to the Defense Security Services (“DSS”).

second sentence of proposed section 204.7301. Consequently, we believe that it would be more correct to use the term "export" than the term "transfer" as the term "export" clearly covers the type of transfers described.

20. Based on all of the above, we suggest that proposed § 204.7301 be amended to read as follows (proposed additional language is underlined and deleted language is struck through):

204.7302 General

Export control laws and regulations ~~restrict the transfer~~ prohibit the unauthorized export, by any means, of certain types of information and technology. The release of technical data subject to the EAR to a foreign national in the U.S., or the disclosure or transfer of technical data subject to the ITAR to a foreign person in the U.S. ~~Any access to export-controlled information or technology by a foreign national or a foreign person anywhere in the world, including the United States,~~ is considered an export to the home country of the foreign national or foreign person. For additional information relating to the restrictions on export-controlled information and technology, see PGI 204.7302.

Proposed § 204.7303 Policy

21. Proposed section 204.7303 provides:

The contracting officer shall ensure that contracts identify any export-controlled information and technology, as determined by the requiring activity.

22. We suggest that the purpose of the proposed rules should not be to identify export-controlled technology in contracts. The identification of technology does not really have any beneficial result. We suggest instead that the purpose of the proposed rules should be to have the contracting officer ensure that the contractor is aware that

the contractor must comply with the export control laws and regulations and that the technology and information involved in the performance of the contract may be subject to export control law and regulation.

23. We are concerned that a focus on identification of the controlled technology will be an impossible requirement for the contracting officer and the contractor. Modern DoD procurements can involve extremely complicated systems that involve thousands or even millions of parts and technologies. To identify all of the export-controlled information and technology at the outset of the program contract, unless in a very general fashion, would involve an incredible amount of efforts and probably would have to be amended continuously through the program life to be accurate.

24. There also is the question of what happens if the list of identified export-controlled export controlled information and technology is either more extensive or less extensive than what is actually required to be licensed by BIS and/or DDTC. We see no benefit to such a requirement.

25. We suggest that Section 204.7303 be replaced by the following, which we believe is a better policy for the proposed rules:

204.7303 Policy

The contracting officer shall ensure that contracts identify the requirement of the contractor to comply with all export control laws and regulations that apply to the contracted activities ~~any export-controlled information and technology,, as determined by the requiring activity.~~

Proposed § 252.204.70XX

26. Paragraph (a) – This paragraph sets for a definition for the phrase “export controlled information and technology” as follows:

(a) Definition. Export-controlled information and technology, as used in this clause, means information and technology that may only be released to foreign nationals or foreign persons in accordance with the Export Administration Regulations (15 CFR parts 730-774) and the International Traffic in Arms Regulations (22 CFR parts 120-130), respectively.

27. We suggest that the scope of the proposed definition is too narrow. As proposed, the rule gives the impression that the scope of the regulations is limited to deemed exports to foreign nationals and foreign persons. The scope of the rule and therefore the scope of the definition should be to cover all unauthorized exports, because that is the scope of the EAR and the ITAR.

28. We suggest the adoption of a different definition of the phrase “export controlled information and technology” that more closely matches the EAR and the ITAR. In fact, we believe it would be more precise and more correct to use the terminology in the EAR and the ITAR. Consequently, we propose amending proposed paragraph (a) as follows:

(a) Definition. Export-controlled information and technology, as used in this clause, means ~~information and technology that may only be released to foreign nationals or foreign persons in accordance with~~ “technical data” as defined in the Export Administration Regulations (15 CFR ~~parts 730-774~~ 772) and “technical data” as defined in the International Traffic in Arms Regulations (22 CFR ~~§120.10)parts 120-130~~), respectively.

29. Paragraph (b) – Proposed paragraph (b) reads as follows:

(b) In performing this contract, the Contractor may gain access to export-controlled information or technology.

30. We can not imagine a situation, other than the supply of such routine items as office equipment, where the Contractor would not have export controlled information or technology related to the products being provided. Furthermore, gaining access to export-controlled information or technology is only one element of the equation. Contractors more than likely already possess export-controlled information and technology at the time of the contract. Contractors also may produce or invent export-controlled information and technology during the contract or may acquire export controlled information and technology from third parties or their subcontractors. Of course, Contractors also may acquire export-controlled information and technology from the Government.

31. The point is not that the Contractor has or acquires export-controlled information and technology but that the Contractor needs to ensure that if the performance of the Contract requires the export of such information or technology (including deemed exports to the Contractor's foreign national employees), then the Contractor must be aware of the need for these exports.

32. Consequently, we suggest that paragraph (b) be amended as follows:

(b) In performing this contract, export-controlled information or technology in the possession of the Contractor may ~~gain access to export-controlled information or technology~~ need to be exported in order to satisfactorily deliver the goods or perform services contracted and that the Contractor may need authorization from the appropriate licensing authority

before any such export-controlled information or technology is exported.

33. Paragraph (c) – Proposed paragraph (c) reads as follows:

(c) The Contractor shall comply with all applicable laws and regulations regarding export-controlled information and technology, including registration in accordance with the International Traffic in Arms Regulations.

34. Not all contractors are required to register with the Department of State, Directorate, Defense Trade Controls (“DDTC”). Contractors to DoD may include manufacturers of dual-use articles and foreign-based manufacturers. There is no requirement for manufacturers or exporters of dual-use equipment to register with DDTC. There also is no requirement for foreign manufacturers to register with DDTC. The requirement to register with the DDTC is limited to U.S. manufacturers and U.S. exporters of “defense articles”.⁸

35. The proposed language does include the use of the term “applicable laws and regulations” and, if properly construed, may not impose a requirement to register with DDTC on a contractor that otherwise would not be required to register with DDTC. Nevertheless, we are concerned that the correct interpretation of this provision may require a level of familiarity with the ITAR that may not exist for most contract officers

⁸ ITAR § 122.1 (17 CFR § 122.1) provides:

(a) Any person who engages in the United States in the business of either manufacturing or exporting defense articles or furnishing defense services is required to register with the Office of Defense Trade Controls. Manufacturers who do not engage in exporting must nevertheless register.

(for both government and industry). This concern becomes particularly acute if this clause is included in subcontracts or is applied to foreign contractors or subcontractors.

36. Therefore, we propose the following clarifying amendment to paragraph (c):

(c) The Contractor shall comply with all applicable laws and regulations regarding export-controlled information and technology, including registration by any person who engages in the United States in the business of either manufacturing or exporting defense articles or furnishing defense services in accordance with the International Traffic in Arms Regulations.

37. Paragraph (d) – Proposed paragraph (d) reads as follows:

(d) The Contractor shall maintain an effective export compliance program. The program must include adequate controls over physical, visual, and electronic access to export-controlled information and technology to ensure that access by foreign firms and individuals is restricted as required by applicable Federal laws, Executive orders, and regulations.

(1) The access control plan shall include unique badging requirements for foreign nationals and foreign persons and segregated work areas for export-controlled information and technology.

(2) The Contractor shall not allow access by foreign nationals or foreign persons to export-controlled information and technology without obtaining an export license, other authorization, or exemption.

38. We suggest that there are numerous problems with paragraph (d) as proposed, particularly if paragraph (d) is going to be required in subcontracts. Furthermore, the language does not make much sense when applied to foreign contractors or foreign subcontractors. These issues are elaborated in the following paragraphs.

39. What is the meaning of the term “effective” and who is going to be the judge of whether the contractor has an “effective export compliance program”? Are all contracting officers going to have the expertise in the EAR and ITAR so that they can determine if a particular compliance program is “effective” or not? What is the objective criteria for making a determination of whether a particular export compliance program is “effective”?

40. Currently, there is no requirement under the ITAR or the EAR that a company have an export compliance program. Does DoD intend to impose a new requirement that does not exist under EAR or ITAR? What is the authority for this requirement?

41. BIS and DDTC highly recommend that companies have a compliance program and both BIS and DDTC have recommendations for the elements of a compliance program.⁹ If a company has a compliance program that has the elements recommended by BIS and/or DDTC, is the compliance program *prima facie* “effective”? Are the requirements in paragraph (d) in addition to the elements recommended by BIS and/or DDTC? If so, what are the additional elements?

42. Paragraph (d) uses the term “access” and thereby introduces terminology that is not used in either the EAR or the ITAR. The correct term for determining if an export has taken place is whether technical data subject to the EAR has been “released” to a

⁹ See, the BIS Export Management System Guidelines at <http://www.bxa.doc.gov/exportmanagementsystems/EMSGuidelines.html> and DDTC Compliance Program Guidelines at http://www.pmdtc.org/docs/compliance_programs.pdf.

foreign national¹⁰ or whether technical data subject to the ITAR has been “disclosed” or “transferred” to a “foreign person” (as defined by ITAR).¹¹ Strictly speaking, the phrase in the proposed paragraph that “access” is “restricted as required by applicable Federal laws, Executive orders, and regulations” is not correct.

43. We suggest that paragraph (d) should be amended to use the wording found in the EAR and the ITAR: the unauthorized release of technical data subject to the EAR is prohibited by law and regulation and that unauthorized disclosure or unauthorized transfer of technical data subject to the ITAR is prohibited by law and regulation.

44. We suggest that it would be unwise to use language that is not the same as the language used in the EAR and/or the ITAR. The introduction of new or different language creates the possibility that a contractor could be found to be in breach of the contract terms but not be in violation of the export control laws and regulations that the contract terms are intended to further.

45. What is the meaning of the term “adequate” and who will determine whether a given export compliance program has “adequate” controls? What are the objective criteria for making such a determination?

¹⁰ See, EAR § 734.2(b)(2) (17 CFR § 734.2(b)(2)). BIS defines the term “release” at EAR § 734.2(b)(3) (17 CFR § 734.2(b)(3)). The term “foreign national” is not defined.

¹¹ The terms “disclosing” and “transferring” are not defined in the ITAR. The term “foreign person” is defined in ITAR § 120.16 (22 CFR § 120.16).

46. If a contractor has a compliance program that has the control elements recommended by BIS and/or DDTC, are the controls *prima facie* “adequate”? Are the requirements in paragraph (d) in addition to the elements recommended by BIS and/or DDTC? If so, what are the additional elements?

47. Subparagraph (1) assumes a requirement that is not stated in the proposed rule that a required element of an export compliance program is an “access control plan.” Again, “access” is not a term used in the EAR or the ITAR. We suggest that instead of an “access” control plan, DoD require a “Technology Control Plan.” Many contractors have Technology Control Plans and must submit a Technology Control Plan with every foreign national employee DSP-5 application.¹²

48. Subparagraph (1) also requires “unique” badging requirements for foreign nationals or foreign persons. We have no idea what the term “unique” means in this context. We assume that what is intended is that foreign nationals be identified by badges so that export-controlled information or technology is not exported inadvertently because the foreign status of the person was not known. However, one must be careful when drafting such requirement not to contravene employment and anti-discrimination laws. This is a very important issue to consider for foreign contractors and subcontractors. We believe this issue can be avoided if stated as a requirement to have badging to avoid unauthorized exports, reexports or retransfers of technical data and

¹² See, DDTC Agreement Guidelines at page 43, http://www.pmdtc.org/ag_guidelines.htm

leave the details of implementation to be worked out in compliance with local employment and anti-discrimination laws and regulations.

49. For all of the above reasons, we believe that it would be preferable to replace the proposed language with language that requires the contractor to certify awareness of the legal requirements, including the obligation to protect against the unauthorized export, reexport or retransfer of technical data. We believe these proposed revisions apply equally well to U.S. and foreign prime contractors and subcontractors. The proposed revisions also reduce the responsibilities of the contracting officers by eliminating responsibilities they are not trained to handle. The proposed revisions are as follows:

(d) The Contractor shall certify the establishment of a written Technology Control Plan to protect against the export, reexport or retransfer, without authorization, of technical data contrary to the requirements of the EAR or the ITAR. maintain an effective export compliance program. The program must include adequate controls over physical, visual, and electronic access to export controlled information and technology to ensure that access by foreign firms and individuals is restricted as required by applicable Federal laws, Executive orders, and regulations.

(1) The Contractor shall certify that the Technology Control Plant covers, at a minimum, the following topics:

(A) Badging of employees and visitors, to protect against the unauthorized (including inadvertent) exports, reexports or retransfers of technical data,

(B) Physical and electronic security of the storage, handling, usage and transmission of technical data,

(C) Initial and periodic export compliance training of employees, and

(D) Periodic export control law and regulation compliance assessments. The access control plan shall include unique badging requirements for foreign nationals and foreign

~~persons and segregated work areas for export-controlled information and technology.~~

~~(2) The Contractor shall not allow access by foreign nationals or foreign persons to export-controlled information and technology without obtaining an export license, other authorization, or exemption.~~

50. Paragraph (e) – We have no objections to the proposed requirement for a Contractor to conduct initial and periodic export control training and to perform periodic compliance assessments. We also believe that it is appropriate to require these provisions to be included in subcontracts. However, we believe that these subjects should be included in the Technology Control Plan contained in the language proposed for paragraph (d) above.

51. Paragraph (f) – No comment.

52. Paragraph (g) – DoD should carefully consider the ramifications of requiring that the proposed clause be included in all subcontracts. It is unclear whether all requirements must be included in subcontracts and to what level of subcontracting this requirement applies. The amendments that have been proposed above, however, appear to work when applied both to foreign contractors and to subcontractors.

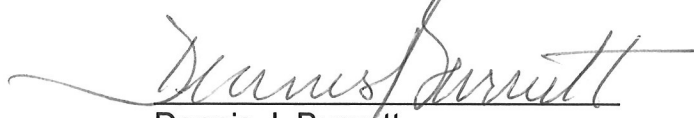
Conclusion

53. EADS North America Defense Company encourages DoD to consider the need for the proposed clause in light of the existence of the EAR and ITAR and the licensing, compliance and enforcement functions of the BIS and DDTC. We suggest that the civil

and criminal penalties available to BIS and DDTC under the EAR and ITAR (respectively) are sufficient to achieve the regulatory objectives without additional contract clauses.

54. If DoD is not persuaded that compliance with export control laws and regulations should not be made part of the terms of DoD contracts, then we urge the consideration of the comments and suggestions to the proposed Parts 204, 135 and 252 as set forth above.

Respectfully submitted,

A handwritten signature in dark ink, appearing to read "Dennis J. Burnett", is written over a horizontal line.

Dennis J. Burnett
V.P. Trade Policy and Export Control
Phone: (703) 236 7538
Fax: (703) 236 7506

September 12, 2005